(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 769 736**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 12703**

(51) Int Cl[6] : G 07 F 7/08

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 10.10.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 16.04.99 Bulletin 99/15.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *PALOS DENIS* — FR et *PALOS AGNES* — FR.

(72) **Inventeur(s) :** PALOS DENIS et PALOS AGNES.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREESE MAJEROWICZ.

(54) PROCEDE POUR LA SECURISATION DE TRANSACTIONS FINANCIERES, CARTE ET TERMINAL DE PAIEMENT METTANT EN OEUVRE CE PROCEDE.

(57) Procédé pour la sécurisation de transactions financières mettant en oeuvre une carte de paiement à mémoire comportant les étapes de saisie d'un code confidentiel par une personne habilitée à utiliser la carte à mémoire et une étape de vérification du code saisie avec des informations préenregistrées dans la carte à mémoire comportant une étape de test déclenchant dans une circonstance prédéfinie l'activation d'une étape de demande d'introduction d'un second code, et de vérification dudit second code.

FR 2 769 736 - A1

2769736

Procédé pour la sécurisation de transactions financières, carte et terminal de paiement mettant en oeuvre ce procédé.

La présente invention concerne le domaine des transactions financières en ligne.

On connaît dans l'état de la technique les transactions financières mettant en oeuvre une carte à mémoire et un terminal de paiement électronique ou un distributeur de billets de banques.

Pour s'authentifier, l'utilisateur détenteur de la carte saisit un code confidentiel avant de pouvoir valider la transaction financière. Dans le cas où le code introduit est erroné, la transaction ne peut s'effectuer.

Ce mode de sécurisation permet de limiter considérablement les fraudes, car il n'est possible d'utiliser la carte à mémoire d'une personne habilitée que si l'on est en possession simultanément du support matériel, et du code confidentiel. La détention de la carte seule ne permet pas de réaliser une transaction financière. De même, la détention du seul code ne permet pas non plus de réaliser une transaction.

Toutefois, il arrive qu'un tiers indélicat obtienne par une indiscrétion le code confidentiel, et s'empare de la carte à mémoire. Il peut alors effectuer des transactions financières au détriment du possesseur de la carte, ou de l'organisme financier de ce dernier.

Le but de l'invention est de remédier à cet inconvénient, par un procédé pour la sécurisation de transactions financières mettant en oeuvre une carte de paiement à mémoire comportant les étapes de saisie d'un code confidentiel par une personne habilitée à utiliser la carte à mémoire et une étape de vérification du code saisie avec des informations préenregistrée dans la carte à mémoire, caractérisé en ce qu'il comporte une étape de test déclenchant dans une circonstance prédéfinie l'activation d'une étape de demande d'introduction d'un second code, et de vérification dudit second code.

De préférence, l'étape de test est une comparaison entre le montant d'une transaction avec une valeur-seuil.

Il apparaît en effet au vue de l'histogramme des transactions d'un utilisateur donné, qu'une très grande majorité de transactions correspondent à une valeur inférieure une valeur-seuil, alors que les transactions abusives sont généralement effectuées pour des montants élevés, et souvent supérieurs à la valeur-seuil.

En imposant la saisie d'un deuxième code pour les transactions correspondant à une valeur inférieure une valeur-seuil, et pour ces montants seulement, on évite que l'utilisateur habilité ne soit obligé de saisir trop souvent deux codes, et surtout on évite qu'une personne indiscrète n'ait accès facilement à ce deuxième code. Par contre, la personne indélicate qui aura volé une carte ne pourra l'utiliser que pour des transactions portant sur de faibles montants.

Selon une première variante, la valeur-seuil est préenregistrée dans la mémoire de la carte de paiement.

Selon une deuxième variante, la valeur-seuil est calculée dynamiquement lors de chaque transaction en fonction des montants des transactions précédentes et est mémorisée dans la mémoire de la carte de paiement.

Avantageusement, la valeur-seuil est calculée de façon à ce que le nombre de transactions dont le montant est inférieur à ladite valeur-seuil soit très supérieur au nombre de transactions dont le montant est supérieur à ladite valeur-seuil.

L'invention concerne également une carte de paiement pour la mise en oeuvre d'un tel procédé caractérisé en ce qu'elle comporte une mémoire permettant d'enregistrer d'une part un premier code confidentiel et d'autre part un second moyen de vérification de l'utilisateur en cas de détection d'une transaction dont le montant dépasse une valeur-seuil.

L'invention concerne également un terminal de paiement pour la mise en oeuvre d'un tel procédé caractérisé en ce qu'il comporte une mémoire permettant d'enregistrer

d'une part un premier code confidentiel et d'autre part un second moyen de vérification de l'utilisateur en cas de détection d'une transaction dont le montant dépasse une valeur-seuil.

L'invention sera décrite dans ce qui suit à titre d'exemple non limitatif.

La carte à mémoire comporte une mémoire dans laquelle sont enregistrées des informations permettant de vérifier le code saisie par un utilisateur sur un terminal de paiement, et de valider la transaction demandée si le code saisie est conforme.

Lorsque la transaction dépasse un montant prédéterminé, la mémoire de la carte déclenche une étape de vérification supplémentaire, consistant à comparer un second code avec une seconde série d'informations enregistrées dans la mémoire de la carte.

La valeur seuil peut être préenregistrée par l'organisme financier délivrant la carte, ou encore par l'utilisateur lui-même. Elle peut également être calculée dynamiquement, de façon à ce que le nombre de transactions dont le montant est inférieur à la valeur-seuil soit très supérieur au nombre de transactions dont le montant est supérieur à la valeur-seuil. A titre d'exemple, la valeur-seuil est déterminée de façon à ce que 80 % des transactions soit effectuées pour un montant inférieur à la valeur-seuil.

La demande de saisie du second code peut également être activée aléatoirement, ou lorsque d'autres circonstances particulières sont détectées, par exemple une succession anormale de saisies incorrectes du premier code.

L'invention n'est pas limité aux exemples de réalisation qui précède, mais peut s'étendre à toute variante de mise en oeuvre.

REVENDICATIONS

1 - Procédé pour la sécurisation de transactions financières mettant en oeuvre une carte de paiement à mémoire et un terminal de paiement électronique comportant les étapes de saisie d'un code confidentiel par une personne habilitée à utiliser la carte à mémoire et une étape de vérification par le terminal de paiement électronique du code saisie avec des informations préenregistrées dans la carte à mémoire, caractérisé en ce qu'il comporte une étape de test déclenchant dans une circonstance prédéfinie l'activation d'une étape de demande d'introduction d'un second code, et de vérification dudit second code.

2 - Procédé pour la sécurisation de transactions financières selon la revendication 1 caractérisé en ce que l'étape de test est une comparaison entre le montant d'une transaction avec une valeur-seuil.

3 - Procédé pour la sécurisation de transactions financières selon la revendication 2 caractérisé en ce que la valeur-seuil est préenregistrée dans la mémoire de la carte de paiement.

4 - Procédé pour la sécurisation de transactions financières selon la revendication 3 caractérisé en ce que la valeur-seuil est calculée dynamiquement lors de chaque transaction en fonction des montants des transactions précédentes et est mémorisée dans la mémoire de la carte de paiement.

5 - Procédé pour la sécurisation de transactions financières selon la revendication 4 caractérisé en ce que la valeur-seuil est calculée de façon à ce que le nombre de transactions dont le montant est inférieur à ladite valeur-seuil soit très supérieur au nombre de transactions dont le montant est supérieur à ladite valeur-seuil.

6 - Carte de paiement pour la mise en oeuvre du procédé conforme à l'une au moins des revendications précédentes caractérisé en ce qu'elle comporte une mémoire permettant d'enregistrer d'une part un premier code confidentiel et d'autre part un second moyen de vérification de l'utilisateur en cas de détection d'une transaction dont le montant dépasse une valeur-seuil.

7 - Terminal de paiment pour la mise en oeuvre du procédé conforme à l'une au moins des revendications précédentes caractérisé en ce qu'il comporte une mémoire permettant d'enregistrer d'une part un premier code confidentiel et d'autre part un second moyen de vérification de l'utilisateur en cas de détection d'une transaction dont le montant dépasse une valeur-seuil.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2769736

N° d'enregistrement national

FA 552378
FR 9712703

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y A	EP 0 440 549 A (GEMPLUS CARD INTERNATIONAL) 7 août 1991 * le document en entier *	1,6,7 2,3,5
Y	GB 2 104 696 A (AMERICAN DISTRICT TELEGRAPH) 9 mars 1983 * abrégé; revendications *	1,6,7
A	EP 0 232 058 A (FUJITSU) 12 août 1987	
A	EP 0 775 990 A (FUJITSU) 28 mai 1997	
A	GB 2 067 467 A (D. EASTWOOD) 30 juillet 1981	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F
G07C

1

Date d'achèvement de la recherche: 7 septembre 1998

Examinateur: David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

FR2769736

Method for securing financial transactions using smart card

Patent Number: FR2769736
Publication date: 1999-04-16
Inventor(s): PALOS AGNES;; PALOS DENIS
Applicant(s): PALOS DENIS (FR)
Requested Patent: FR2769736
Application Number: FR19970012703 19971010
Priority Number(s): FR19970012703 19971010
IPC Classification: G07F7/08
EC Classification: G07F7/10D6P, G07F7/10D4T
Equivalents:

Abstract

The transaction security method captures a confidential access code entered by the presenter of the smart card. In certain circumstances, such as transactions above a particular value, a second confidential code is required to provide verification of the first code. The threshold may be pre-stored in the card, or computed dynamically from an average of previous transactions.

Description

Process for the securisation of financial transactions, card and terminal of payment implementing this process.

The present invention relates to the field of the financial transactions on line.

One knows in the state of the art the financial transactions implementing a smart card and an electronic payment terminal or a banknote distributor.

To authenticate itself, the user holder of the card seizes a confidential code before being able to validate the financial transaction. If the introduced code is erroneous, the transaction cannot be carried out.

This mode of securisation makes it possible to limit the frauds considerably, because it is not possible to use the smart card of a person competent but if one is in possession simultaneously material support, and confidential code. The detention of the card alone does not make it possible to carry out a financial transaction. In the same way, the detention of the only code does not make it possible either to carry out a transaction.

However, it happens that an indelicate third obtains by an indiscretion the confidential code, and seizes the smart card. It can then carry out financial transactions with the detriment of, or the financial organization card holder of this last.

The goal of the invention is to cure this disadvantage, by a process for the securisation of financial transactions implementing a card of payment at memory comprising the stages of data entry of a confidential code by a person entitled to use the smart card and a stage of checking of the code seized with information preregistered in the smart card, characterized in that it comprises a stage of test starting in a preset circumstance the activation of a stage of request for introduction of a second code, and of checking of the aforesaid second code.

Preferably, the stage of test is a comparison between the amount of a transaction with a threshold value.

It indeed appears with the sight of the histogram of the transactions of a given user, that a very large majority of transactions correspond to a value a lower threshold value, whereas the abusive transactions are generally carried out for raised amounts, and often higher than the threshold value.

By imposing the data entry of a second code for the transactions to a value a lower threshold value corresponds, and for these amounts only, one prevents that the competent user is not obliged to too often seize two codes, and especially one avoids qu wse nobody indiscreet does not have access easily to this second code. On the other hand, the indelicate person who will have stolen a card will be able to use it only for transactions carrying surde weak amounts.

According to a first alternative, the threshold value is preregistered in the memory of the card of payment.

According to a second alternative, the threshold value is calculated dynamically at the time of each transaction according to the amounts of the preceding transactions and is memorized in the memory of the card of payment.

Advantageously, the threshold value is calculated so that the number of transactions whose amount is lower than the aforementioned threshold value is much higher than the number of transactions whose amount is higher than the aforementioned threshold value.

The invention also relates to a card of payment for the implementation of such a process characterized in that it comprises a memory making it possible to record on the one hand a first confidential code and on the other hand a second means of checking of the user in the event of detection of a transaction whose amount exceeds a threshold value.

The invention also relates to a terminal of payment for the implementation of such a process characterized in that it comprises a memory making it possible to record on the one hand a first confidential code and on the other hand a second means of checking of the user in the event of detection of a transaction whose amount exceeds a threshold value.

The invention will be described in what follows as an example nonrestrictive.

The smart card comprises a memory in which information is recorded making it possible to check the code seized by a user on a terminal of payment, and to validate the asked transaction whether the code seized is in conformity.

When the transaction exceeds a predetermined amount, the memory of the card starts a stage of checking supplimentaire, consisting in comparing a second code with one second data recorded in the memory of the card.

The value threshold can be preregistered by the financial organization delivering the card, or by the user himself. It can also be calculated dynamically, so that the number of transactions whose amount is lower than the threshold value is much higher than the number of transactions whose amount is higher than the threshold value. As an example, the valeurseuil is given so that 80 % of the transactions are carried out for an amount lower than the threshold value.

The request for data entry of the second code can also be activated by chance, or when other particular circumstances are detected, for example an abnormal succession of incorrect data entries of the first code.

The invention is not limited to the examples of realization which precedes, but can extend to any alternative from implementation.

CLAIMS

1 - Proceeded for the sécurisation of financial transactions implementing a payment card to memory and a final one of electronic payment including the seizure steps of a confidential code by an empowered person to use the smart card and a verification step by the final one of electronic payment of the seized code with information preregistered in the smart card, characterized in this step of test starting in a preset circumstance the activation of a request step of introduction of a second code, and of verification aforesaid second code.

2 - Proceeded for the sécurisation of financial transactions according to claim 1 characterized one in this that the step of test is a comparison between the amount of a transaction with a threshhold value.

3 - Proceeded for the sécurisation of financial transactions according to claim 2 characterized in that the threshhold value is preregistered in the memory of the payment card.

4 - Proceeded for the sécurisation of financial transactions according to claim 3 characterized in that the threshhold value dynamically is calculated at the time of every transaction according to the amounts of the preceding transactions and is memorized in the memory of the payment card.

5 - Proceeded for the sécurisation of financial transactions according to claim 4 characterized in that the threshhold value is calculated so that the number of transactions whose amount is lower than the aforementioned value threshhold is much higher than the number of transactions whose amount is higher than the aforementioned threshhold value.

6 - payment Card for the implement procedure in accordance with at least of the preceding claims characterized in that it comprises a memory making it possible to record on the one hand a first confidential code and on the other hand a second means of verification of the user in case of detection of a transaction whose amount exceeds a threshhold value.

7 - Final of payment for the implement procedure in accordance with at least of the preceding claims characterized in that it includes a memory allowing to record on one hand a first confidential code and on the other hand a second of verification of the user in case of detection of a transaction whose amount exceeds a threshhold value.